



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/611,832

06/30/2003

Art Shelest

13768.344

3053

47973

7590

11/16/2006

WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER

CERVETTI, DAVID GARCIA

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 11/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/611,832

Applicant(s)

SHELEST ET AL.

Examiner

David G. Cervetti

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 June 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-51 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-51 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 June 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>6/30/03</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-51 are pending and have been examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 1 and 23 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. It is not clear where the firewall is sending the firewall credentials.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. **Claims 23-44 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.**

Claims 23 and 34 are not limited to tangible embodiments. In view of applicant's disclosure, specification pages 21-22, the medium is not limited to tangible embodiments, instead being defined as including both tangible embodiments (e.g., RAM, CD-ROM, other storage) and intangible embodiments (e.g., wireless, wired

connection). As such, the claim is not limited to statutory subject matter and is therefore non-statutory.

Claims 24-33 and 35-44 are rejected based on their dependency from independent claims 23 and 34 respectively.

6. To expedite a complete examination of the application, the claims rejected under 35 U.S.C. 101 (non-statutory) above are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. **Claims 1-51 are rejected under 35 U.S.C. 102(b) as being anticipated by Check Point (NPL “Check Point FireWall-1 User Guide”, books “Architecture and Administration” – AA, and “Virtual Private Networking with Check Point FireWall-1” – VP, hereinafter Checkpoint).**

Regarding claims 1 and 23, Checkpoint teaches in a private network comprising a resource and a firewall, which acts as a gateway by controlling client desired access to the private network resource, a method of establishing a connection to the private network resource while balancing authentication processing requirements

between a client and the firewall to mutually guard against denial of service attacks (**AA, chapter 1, pp. 28-41**), the method comprising the acts of:

- receiving, by the firewall, a request from the client to access the private network resource, wherein the request from the client is made to the private network resource without any knowledge of the firewall (**AA, chapter 1, pp. 27-29**);
- requesting, by the firewall, the client to provide one or more client credentials to authenticate the client (**AA, chapter 1, pp. 30-34**);
- sending, by the firewall, one or more firewall credentials to authenticate the firewall, wherein generating the one or more firewall credentials consumes some level of limited firewall processing resources (**AA, chapter 1, pp. 35-39**);
- receiving one or more client credentials at the firewall, wherein generating the one or more client credentials consumes some level of limited client processing resources similar in magnitude with the consumption of the limited firewall processing resources (**AA, chapter 1, pp. 39-48**);
- verifying, by the firewall, the one or more client credentials (**AA, chapter 1, p. 28**);
- establishing a secure channel for accessing the private network resource in response to the verification of the one or more client credentials (**VP, chapter 1, pp. 11-13, chapter 2, pp. 11-20**); and

- forwarding data from the client destined to the private network resource through the firewall using the secure channel (**AA, chapter 1, pp. 27-29, VP, chapter 2, pp. 22-34**).

Regarding claims 12 and 34, Checkpoint teaches in a private network comprising a resource and a firewall, which acts as a gateway by controlling client desired access to the private network resource, a method of establishing a connection to the private network resource while balancing authentication processing requirements between a client and the firewall to mutually guard against denial of service attacks (**AA, chapter 1, pp. 28-41**), the method comprising steps for:

- initiating a series of authentication transactions designed to impose commensurable processing burdens on the client requesting access to the private network resource and the firewall operating as a gateway for the private network, wherein the client initially is unaware that the firewall operates as a gateway for the private network, and wherein each authentication transaction incrementally increases a level of trust between the client and the firewall until the authentication of the client and the firewall are sufficiently verified (**AA, chapter 1, pp. 28-41**);
- for each of the series of authentication transactions:
- authenticating to the client in accordance with one of the series of authentication transactions (**AA, chapter 1, pp. 39-48**); and
- challenging the client to authenticate in a manner requiring similar processing burdens (**AA, chapter 1, pp. 39-48**); and

- granting the client access to the private network resource through the firewall upon completing the series of authentication transactions (**AA, chapter 1, pp. 28-48**).

Regarding claim 45, Checkpoint teaches in a private network comprising a server and a firewall, which acts as a gateway by controlling access to the server, a method of providing access to the server through the firewall without a client knowing about the firewall (**AA, chapter 1, pp. 28-41**), the method comprising the acts of:

- receiving at the firewall, an access request from the client that is directed to the server because the client does not know that the firewall operates as a gateway for the server (**AA, chapter 1, pp. 27-29**);
- generating one or more authentication credentials at the firewall that demonstrate a level of trust between the server and the firewall (**AA, chapter 1, pp. 28-34**);
- the firewall sending a request for the client to authenticate to the firewall, the request including the one or more firewall authentication credentials so that the client knows of the level of trust between the server and the firewall without having to make a separate request (**AA, chapter 1, pp. 35-39**);
- receiving at the firewall, one or more authentication credentials from the client (**AA, chapter 1, pp. 27-39**);
- the firewall verifying the one or more client authentication credentials (**AA, chapter 1, p. 28**); and

- thereafter, allowing the client to access the server through the firewall (**AA, chapter 1, p. 28**).

Regarding claims 2 and 24, Checkpoint teaches wherein the step of verifying comprising the act of: continuing an exchange of credentials between the client and the firewall to incrementally increase a level of trust between the client and the firewall until a predefined threshold of trust is reached (**AA, chapter 1, pp. 27-33**).

Regarding claims 3, 19, 25, 41, and 48, Checkpoint teaches wherein the private network resource is one of a host, gateway or server (**AA, chapter 1, pp. 27-33**).

Regarding claims 5, 22, 27, and 44, Checkpoint teaches establishing a connection with a resource of a separate private network while simultaneously maintaining the secure channel of the private network (**VP, chapter 1, pp. 11-13**).

Regarding claims 6, 21, 28, and 43, Checkpoint teaches establishing a connection with another private network resource while simultaneously maintaining the secure channel of the private network (**VP, chapter 1, pp. 11-13**).

Regarding claims 7, 17, 29, and 39, Checkpoint teaches wherein the act of forwarding the data from the client to the private network resource is accomplished through the use of an authenticated channel, the method further comprising the act of: signing, by the firewall, the packets of data from the client destined to the private network resource, wherein the signing indicates that the client has passed one or more security check implemented in the firewall (**VP, chapter 1, pp. 7-13**).

Regarding claims 8, 18, 30, and 40, Checkpoint teaches discarding unsigned packets of data received by the protected private network resource (**VP, chapter 1, pp. 7-13**).

Regarding claims 11, 20, 33, 42, and 49, Checkpoint teaches wherein the client is a second firewall (**AA, chapter 1, pp. 27-29**).

Regarding claims 13 and 35, Checkpoint teaches wherein the step for challenging the client to authenticate comprises the acts of: requesting, by the firewall, the client to provide one or more client credentials; receiving one or more client credentials at the firewall; and verifying, by the firewall, the one or more client credentials (**AA, chapter 1, pp. 27-33**).

Regarding claims 9, 14, 31, and 36, Checkpoint teaches wherein the one or more client credential received is selected from at least one of a user's name, client's IP address, password, passport, smart-card or credit card number (**AA, chapter 1, pp. 27-33**).

Regarding claims 10, 15, 32, and 37, Checkpoint teaches wherein the request, by the firewall, for the client to provide one or more client credentials is a question, and wherein the one or more client credentials received is an answer to the question (**AA, chapter 1, pp. 29-33**).

Regarding claims 4, 16, 26 and 38, Checkpoint teaches wherein the only data passed through the firewall from the client are those packets of data destined to the private network resource (**AA, chapter 1, pp. 27-33**).

Regarding claims 46, Checkpoint teaches establishing a secure connection between the firewall and the server; and forwarding data received from the client to the server over the secure connection (**AA, chapter 1, pp. 27-33**).

Regarding claim 47, Checkpoint teaches receiving at the firewall data from the client; the firewall signing the received data; and the firewall forwarding the signed data to the server (**VP, chapter 1, pp. 7-13**).

Regarding claim 50, Checkpoint teaches wherein the client maintains a separate connection with another server (**VP, chapter 1, pp. 11-13**), and wherein only data intended for the private network passes through the firewall (**AA, chapter 1, pp. 27-33**).

Regarding claim 51, Checkpoint teaches wherein the other server is part of a separate and distinct virtual private network (**VP, chapter 2, pp. 15-32**).

Conclusion

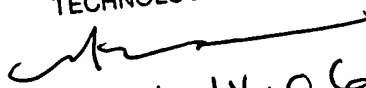
9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

10. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

11. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DGC

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


11/14/06